Research on Security Issues of RFID Technology in IOT

Jin Hong-ying
College of Computer
China West Normal University
Nanchong, Sichuan, China, 13990876161
46840639@qq.com

Tian Min
College of Computer
China West Normal University
Nanchong, Sichuan, China

Abstract— **With the global development of IOT, people are more worried about their personal information security issues. Through the analysis of security problems, this paper introduces symmetric grouping algorithm DES to encrypt the data between tags and readers based on Hash-Lock protocol,. In order to reduce the workload of the backend database, this paper increases a pre-treatment process to judge whether the tag belongs to this database.**

Keywords-IOT; RFID; Hash-Lock protocol; security and privacy; DES algorithm

I. INTRODUCTION

With all the fast growth the new technology, the rapid development of Internet of Things bring convenience and fast as well as a series of safety related problems, especially its building foundation RFID technology. In the RFID system, the communication between the tag and the reader is in an environment which is absolutely have no protection, so all the reader in this open space may receive the information sent over tag, and at the same time ,it is also possible for tag to response more than one reader's request. So it is likely to cause the tag information disclosed or malicious falsified. Further, attacker can also make the unauthorized use of the system by forgery.

II. THE ANALYSIS OF SECURITY THREAT IN THE RFID SYSTEM OF IOT

Basically, there are tow kinds of security and privacy problem in the RFID system. One is tag information leakage another is malicious tracking according to the only electronic coding (EPC) of tags.

A. Information Leakage

Information leakage is the exposure of the information sent by tags, including the information of electronic tag user and recognition object. Because electronic tag can work in any surroundings, the communication between readers and tags is in the unsafe channel without any protection, so tag information disclosure problems are common.

B. Malicious Tracking

The tags of RFID system are usually contain electronic code(EPC)only, users access database on the backend sever through it to get the target's relevant information. Therefore, the attacker can follow up the tag through the only EPC coding. Because the uniqueness of the electronic code, even use the encryption technology in the electronic tag, attackers can still tracking tags through the tracking of fixed cipher text and get the position information of tag users.

III. RFID SYSTEM SECURITY REQUIREMENTS ANALYSIS IN IOT

From the point of view of the data communication, the security and privacy of the RFID system in IOT mainly include the following:

Data confidentiality: radio frequency identification tag can only respond to the reader which is authorized, and for those who are not authorized reader, tags should not disclose any sensitive information.

Data integrity: in the communication process, we should ensure that the information transmitted between the tags and readers is complete and correct, without any tampering and replace. The reliability of the information source and integrity needs effective identification to guarantee. Once the information transmitted under the attack, there should be a corresponding measure can be sure that the destruction of the integrity, and then restore information transmission.

Data authenticity: the attacker can get the sensitive information through tap the communication between the tags and the readers, and reconstruct the RFID tag to forge it. The reader must use message authentication to ensure that message is derived from the right, and the actual tag. Tag can ALSO know that message comes from the true, lawful readers. Therefore, it is necessary for us to use the proper safety measures to ensure the authenticity of the data communication.

High efficiency: the main purpose to use RFID technology in IOT is to improve the speed of each link in the network. If we need to spend a lot of time to realize the security and confidential of the system, it will cause the inefficient of the whole network.

User privacy leak: in IOT, all the information in the tags is related to the user's privacy. Once be acquired by the attacker, this information will cause the user privacy information disclosure.

IV. THE AGAINST MODEL OF RFID SYSTEM IN IOT

The main safety attack means can be divided into two kinds, active attack and passive attack. Active attack is an important safety factor affect the normal use of RFID system. It use the physical or software method to tamper with the tag, and through delete tag content and radio interference or channel obstruction to disturb the normal work of the legal processor. Passive attacks do not change the contents of the RFID tags, will not affect the normal work of the RFID application system. But it is the important means to gain RFID system information， personal privacy and goods information, so it is also the important security hidden danger of RFID system application.

In this paper, we do not consider the physical attack after gain the tag, only from the point of view of information security logic to discuss, and create an against model as the following:

1) *Forgery attack:* the attacker can make a simple copy for tag by get the content of electronic tag.

2) *Replay attack*:the attacker can wiretap the response information of electronic tags and retransmit it to the legal readers.

3) *Middleman attack*:refers to the attacker disguised as a legal device for reading and writing tag response information, and use this information to disguised as a legitimate electronic tags to response for reading and writing. So, before the next round communication, attacker can obtain the authentication of legal reader.

4) *Denial of service attack:*the attacker intercept the information sent by tags,modify it, and then send it to the reader.Reader will send this modified information to the backend servers,backend server need to search and calculate all the tag information stored in the database and identify this tag can not be authenticated.IF the attacker send modified information repeatedly,the system will become paralyzed.

V. PROJECT DESIGN

A. *Project Design Premise*

Consider that we need to reduce the cost of tags, so we use relatively cheap passive tags as RFID system tag. Assume that the tag have been added to the Hash function and DES algorithm declassified circuit, and the Hash function is we need to meet strong collision-free, DES algorithm decryption function is match with the encryption algorithm used in readers. And once the authentication is successful, tag will turn to safe mode only accept the operation of authentication successful reader. In the reader, there must be a DES algorithm encryption circuit, and must store the identifier of backend database and its hash value. The database will be able to realize the dynamic refresh of tag ID, after the two-way authentication it should refresh the tag ID.

B. *Protocol Initialization*

In the initial state, tag stores its own real ID and the identifier P of its database. Reader stores identifier P’ which is match with P and its hash value H(P’).In the backend database, there must be all the ID of tags and the hash value of each ID,H(ID).

C. *Protocol Description*

The execution of this protocol process is shown in Fig.1.

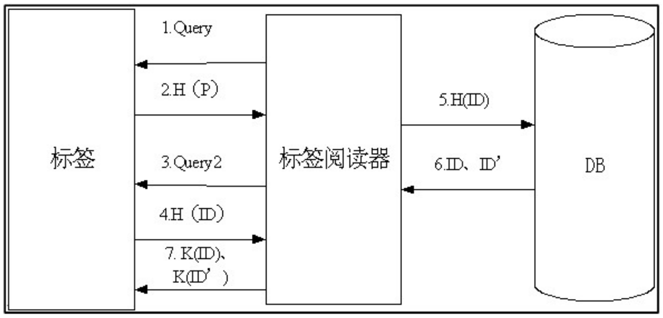

Figure 1. The flow chart of the improved protocol

a) Reader sends the request Query to the tag for verification.

b) Afyter receive the request singnal from the reader, tag calculates the hash value of its database identifier P, and then send the value H(P)to the reader.

c) Reader compare the H(P) with its H(P’), if they are equal, it send further verification Query 2 signal.If they are not equal, it means that tag is not belong to the database system, and the verification stop, send the Query 1 singnal to the next tag.

d) Tag receive the signal Query 2 sent from reader, calculate its ID,and get its hash value,then send it to the reader.

e) Reader send the H(ID) to the backend database.

f) After receive the H(ID), backend database search its database to find out whether a ID_i meet make $H(ID_i)=H(ID)$ is established, if any, tag identity authentication success,and creat a new identity number ID’ for this authenticated tag, store it in a new field in record ID.At last, send both ID_i and ID’ to the reader.Otherwise the authentication failure.

g) Reader receive the ID_i and ID’,encrypt them use the DES algorithm, get the ciphertext $K(ID_i)$ and K(ID’) and send them to the tag.

h) Tag receive the $K(ID_i)$ and K(ID’), decrypt the $K(ID_i)$ to get ID_i, compared with its own ID, if ID_i is equal to ID, the authentication of reader is success, and go on to decrypt the K(ID’) to get ID’, Otherwise the authentication failed.

i) Tag and reader refresh tag ID into ID’ simutaneously. Tag turn into safe mode and can accep the operation of reader.

D. *Protocol Analysis*

1) *Protocol safety analysis：*

a) Data confidentiality: In the original protocol, when use Hash-Lock protocol o realize two-way authentication between tag and reader, the communication between reader and tag is the plaintext in unsafe wireless channel, so it is very vulnerable to be attacked. The improved protocol use the most well-known encryption algorithm DES to encrypt the information transmitted between the reader and the tag. Since it will need relatively long time (at least a few hours) to decrypt the cipher text while the attacker do not know the key used in DES algorithm, so when the attacker get the tag ID after several hours, the real tag ID have already update, and the information the attacker got is useless. So the improved protocol based on Hash-Lock protocol in this paper can protect the data confidentiality.

b)Data integrity and authenticity: The character strong collision-free decides that attacker can not find another ID_j make H(ID)=H(ID) is established, so there is no way for attacker to forge as legitimate tag to tamper the communication information. Even if attacker use what is called middleman attack to forge as reader to receive the information sent by tag and then use this information to forge as tag to communicate with legal reader, because the signal Query 2 is encrypted, for the same reason, when the attacker using poor search approach to crack, tag ID have changed. It can not disguise as a legitimate tag to communicate with backend database, but to waste a lot of manpower.

*c)User privacy protection:*Use this improved protocol o complete the identity authentication and communication process, every time after communication between tag and system is finished, they will refresh their tag ID, thus the attacker can not effectively track the tag, so it can not known the exact physical position of tag carrier, even who have use this tag. So it can effectively realize the user privacy information protection.

*d)Denial of service attacks:*Because before search the database to determine whether this tag belong to the database, the protocol let the reader judge whether the tag is belong to the database, all the tags which is not belong to this system is removed. Therefore can reduce a certain extent calculation for backend database, and reduce the possibility of the denial of service attacks. At he same time the operation of judge tag ownership is moved to tag reader, it makes the backend database do not need to send all the tag ID to the reader every time, but only vivificated the tag which have already finished preliminary judgment. In the environment that a lot of tags coexist, the result is the traffic between reader and backend database greatly reduced, so as to alleviate the problem of safe information channel congestion.

2) *Protocol performance analysis*

According to the reference [2], [6] records, when design a 5 cents tag, integrated circuit chip costs should be no more than 2 cents, this limited the number of integrated circuit between 7.5kb to 15 kb. A 96 bit EPC chip need about the size of 5kb-10kb circuit, so the size of circuit for security and privacy protection should be 2.5kb-5kb.In the improved protocol, tags contain a Hash function calculation, need a 1.7 k gate circuit to achieve, and realizing the declassification of DES algorithm needs a simple circuit, so the solution of this paper can meet the requirements of the lower costs.

Compared with the Hash-Lock protocol, the improved protocol adds the encryption algorithm, so it is relatively added the security of the system. From the perspective of the amount of calculation, because of the need of information encryption, the improved protocol increases the calculation than Has-Lock protocol. But using the identifier of database, reader distinguish whether the tag is belong to the system before the authentication, instead of database search itself for discrimination through hash method, thus greatly reduce the workload of the database. Further, the improved protocol does not need the database send all the tag ID to the reader for each authentication, so it can reduce the traffic between the reader and the database, solve the problem of information security channel congestion, can greatly improve the efficiency of the whole system. Even in the system using huge number of tags, because the workload of backend database is reduced by the reader, the possibility of denial of service attack greatly decreased.

VI. Conclusion

Introduce the DES encryption algorithm for Has-Lock protocol to encrypt the communication data transferred between tag and reader can solve the problem that the information is the plaintext without any protection. By using the pretreatment process module in the reader, the new protocol reduces the workload of the backend database. In order to solve the synchronization problem between tag and the database, the new protocol let tag and database refresh the tag ID simultaneously after the authentication. At the end, this paper analysis the safety and performance of the improved protocol, demonstrates that the new protocol can reduce the cost of the whole system while meet the security request.

References

[1] Security Problems in the Internet of Things and Their Solutions, Peng Yong,XieFeng,GuoXiao-jing,SongDan-jie,LiJian. NetinfoSecurity2011(10)

[2] Hui Yue-chao,The Security Research of Low-Cost RFID system, [D]Su Zhou:Soochow university,2010

[3] The Key Technologies and Primary Urgent Problems of IOT,Du Tian-xu,Xie Lin-bo,Xu Ying-qin, Micro Computer Information,2011.Vol27(5)

[4] ITU Internet Reports 2005: The Internet of Things [EB/OL].[2010-02-15].http://www.itu.int/internetofthings/

[5] Liu-Xiu-li, “ 2010 IOT system research report ” ,[EB/OL]. http://doc.mbalib.com/view/58a981615c0b9d4bf953ab9fee7872bb.html. 2011-2-18.

[6] S. E. Sarma, S. A. Weis, D. W. Engels. Radio frequency identification security risks and Challenges[J]. RSA Laboratories CrptoBytes. 2003, 6(1): 2-9.